## IN THE CLAIMS

Please substitute claims 1-15 with the following:

1. (Currently Amended) A content distribution system for performing content transaction management, comprising:

a plurality of user devices among which the content transaction management allows a content to be secondarily distributed;

a secure container containing the content encrypted by a content key, and container information including conditions set for a transaction of the content;

a first section for distributing the content by transmitting said secure container; and

a second section for performing person authentication, when said secure container is transmitted among said plurality of user devices, based on a person identification certificate (hereinafter, simply referred to as an IDC) which is identified in reference to an IDC identifier list,

wherein the container information includes the IDC identifier list as a list of the IDCs, ~~each of which~~ the IDC identifier list is generated by a person identification authority (hereinafter, simply referred to as an IDA) as a third party agent and stores a template serving as person identification data of a target user for the content transaction,

wherein a secure container distributing device among said plurality of user devices is configured to compare sampling information input by a user with the template stored in the IDC identified in reference to the IDC identifier list, to process person authentication of a user of a receiving device among said plurality of user devices, to which the secure container is to be

distributed, and to perform a process of distribution of the content key for decrypting the content stored in said secure container, when the comparison result is affirmative.

2. (Original) The content distribution system according to Claim 1,

wherein a secure container receiving device among said plurality of user devices generates usage control status information on a content based on the container information included in said secure container, and stores the usage control status information in a memory of the receiving device, and further the usage control status information includes the IDC identifier list.

3. (Original) The content distribution system according to Claim 1,

wherein a secure container receiving device among said plurality of user devices generates usage control status information on a content based on the container information included in said secure container, and stores the usage control status information in a memory of the receiving device, and further the usage control status information includes conditions set for processing secondary distribution of the content after a primary content distribution.

4. (Original) The content distribution system according to Claim 1,

wherein a secure container distributing device among said plurality of user devices is configured to compare sampling information input by a user with the template stored in the IDC identified in reference to the IDC identifier list, to process person authenticiation of a user of a receiving device among said plurality of user devices, to which the secure container is to be distributed, and to perform a process so that a content is available at the receiving device, when the comparison result is affirmative.

5. (Cancelled).

6. (Original) The content distribution system according to Claim 1,

wherein a secure container distributing device among said plurality of user devices is configured to compare sampling information input by a user with the template stored in the IDC identified in reference to the IDC identifier list, to process person authentication of a user of the receiving device, to which the secure container is to be distributed, and to notify a distributing device among said user devices, as a distributor of said secure container, of the process result of the person authentication, and further the distributing device is configured to perform a process so that a content is available at the receiving device, when the comparison result is affirmative.

7. (Original) The content distribution system according to Claim 1,

wherein a secure container distributing device among said plurality of user devices is configured to compare sampling information input by a user with the template stored in the IDC identified in reference to the IDC identifier list, to process person authentication of a user of the receiving device, to which the secure container is to be distributed, and to notify a distributing device among said user devices, as a distributor of said secure container, of the process result of the person authentication, and further the distributing device is configured to perform processes so that said secure container and ~~the~~ said content key stored in said secure container are distributed to the receiving device of said secure container and available at the receiving device, when the comparison result is affirmative.

8. (Original) The content distribution system according to Claim 1,

wherein the IDC used for person authentication, which is performed when said secure container is transmitted among said plurality of user devices, is configured to be stored in advance in any of said plurality of user devices which is to perform the person authentication.

9. (Original) The content distribution system according to Claim 1, wherein any of said user devices, which is to perform person authentication when said secure container is transmitted among said plurality of user devices, is configured to obtain the IDC used for the person authentication from the IDA as an issuer of the IDCs.

10. (Currently Amended) The content distribution system according to Claim 1, wherein the container information further includes usage permission data of the content ~~such as reproduction and duplication of the content~~, and a receiving device among said plurality of user devices is configured to perform restricting usage of the content based on the usage permission data of the content or usage control status information generated according to said usage permission data.

11. (Original) The content distribution system according to Claim 1, wherein said secure container further is configured to include a digital signature of a producer of said secure container.

12. (Original) The content distribution system according to Claim 1, wherein the IDC identifier list is configured to include data for associating a user identifier with his/her IDC identifier.

13. (Original) The content distribution system according to Claim 1, wherein each of distributing and receiving devices among said plurality of user devices, which are to perform a content transaction, further comprises an encryption unit, so that each of the devises is configured to perform mutual authentication upon performing data transmission between the distributing and receiving devices, and further the data transmitting and receiving sides are

configured, respectively, to generate a digital signature of the transmitting data and to verify the digital signature.

14. (Original) The content distribution system according to Claim 1, wherein the template comprises at least any one of the following (a) to (d): (a) personal biotic information including fingerprint information, retina pattern information, iris pattern information, voice print information, and handwriting information; (b) personal non-biotic information including a seal, a passport, a driver's license, and a card; (c) combined information between the biotic information and the non-biotic information; and (d) another combined information of a password and either of (a) and (b).

15. (New) A content distribution system for performing content transaction management, comprising:

a plurality of user devices among which the content transaction management allows a content to be secondarily distributed;

a secure container containing the content always encrypted by a content key, and container information including conditions set for a transaction of the content;

a first section for distributing the content by transmitting said secure container; and

a second section for performing person authentication, when said secure container is transmitted among said plurality of user devices, based on a person identification certificate (hereinafter, simply referred to as an IDC) which is identified in reference to an IDC identifier list,

wherein the container information includes the IDC identifier list as a list of the IDCs, the IDC identifier list is generated by a person identification authority (hereinafter, simply referred

to as an IDA) as a third party agent and stores a template serving as person identification data of a target user for the content transaction.